UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/581,445	06/02/2006	Masao Nonaka	2006_0778A	6614

52349 7590 07/08/2010
WENDEROTH, LIND & PONACK L.L.P.
1030 15th Street, N.W.
Suite 400 East
Washington, DC 20005-1503

EXAMINER	
YANG, JAMES J	
ART UNIT	PAPER NUMBER
2612	
NOTIFICATION DATE	DELIVERY MODE
07/08/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ddalecki@wenderoth.com
eoa@wenderoth.com

Office Action Summary	**Application No.** 10/581,445	**Applicant(s)** NONAKA ET AL.	
	Examiner JAMES YANG	**Art Unit** 2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 April 2010*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,5-15,30,31,35,36,38,39,42,43 and 45-47* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,5-15,30,31,35,36,38,39,42,43 and 45-47* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

This Office Action is in response to applicant's amendment filed 04/27/2010. Claims 1, 5-15, 30-31, 35-36, 38-39, 42-43, and 45-47 are currently pending in this application.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1, 5-7, 12, 31, 36, 39, 43, and 46-47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061).

Claims 1, Ahlstrom teaches:

An authentication system (Ahlstrom, Paragraph [0003]**), comprising:**

an IC card of a forwarding agent (Ahlstrom, Paragraph [0031], A card read by a card reader is a portable recording medium, and the user is a forwarding agent.**);**

an authentication apparatus operable to verify authenticity of a visit by the forwarding agent (Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card.**), the authentication apparatus being provided in a residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph

[0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building. The system can be implemented in a place of residence (see Ahlstrom, Paragraph [0026]).**)** **of a person who is visited by the forwarding agent (**Ahlstrom, Paragraph [0026], Ahlstrom further discloses issuing temporary access cards, which is here interpreted as cards for people who only temporarily need access to the entrance by way of cards (see Paragraph [0035]). Therefore, these people may be interpreted as visitors.**); and**

a card reader operable to perform inputting and outputting of information between the IC card portable recording medium and the authentication apparatus (Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit.**), the card reader being for reading the IC card and being provided at an entrance of the residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building.**),**

wherein the IC card stores in advance at least one piece of information concerning the authenticity of the visit by the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**),**

wherein the authentication apparatus stores at least one piece of information for verifying the authenticity of the visit by the forwarding agent (Ahlstrom, Paragraph [0028]**), and judges whether or not the visit by the forwarding agent is authentic by, via the card reader, performing an authentication using (a)**

the information concerning the authenticity of the visit by the forwarding agent and stored in the IC card, and (b) the information for verifying the authenticity of the visit by the forwarding agent and stored in the authentication apparatus (Ahlstrom, Paragraph [0031]**),**

wherein the IC card stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit by the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. The access codes are thus certification information stored on the IC card that is used to certify authenticity.**),**

wherein the authentication apparatus stores, as the information for verifying the authenticity of the visit by the forwarding agent, authentication information used to examine the certification information (Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card. The authentication apparatus has a list of authorized access codes (see Paragraph [0028]).**),**

wherein the card reader detects a lock status of an entrance door of the residence (Ahlstrom, Paragraphs [0022] and [0030], The system has sensors to detect whether a door is opened or close. It is well-known in the art that doors in a controlled access system are locked when the door is closed, thus the sensors are capable of determining the lock status of the door.**), such that, when the card reader detects that the entrance door is locked, the authentication apparatus performs, via the**

card reader, the authentication using the certification information from the IC card and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic (Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**),**

wherein the IC card further stores, as the information concerning the authenticity of the visit, first visit information that indicates a business of the visit by the forwarding agent (Ahlstrom, Paragraph [0035], Temporary cards are programmed to only work for a certain time period, or for a certain number of times. Thus, the time periods and times are also considered as the business of the visit, because it signifies to the system that the user wants entry to the area in a specified time period The term "business" is here interpreted as meaning "purpose".**),**

wherein the authentication apparatus further stores, as the information for verifying the authenticity of the visit, second visit information used to examine the first visit information (Ahlstrom, Paragraph [0035], The system is programmed to recognize an access code as having time restrictions, thus the access code also serves as information concerning authenticity. The time restrictions are thus second visit information, and the access codes are stored in the main unit (see Paragraph [0028]).**),**

wherein, when a result of the authentication using the certification information from the IC card and the stored authentication information is positive, the authentication apparatus (c) acquires the first visit information from the IC

card via the card reader, (d) judges whether or not the acquired first visit information matches the stored second visit information, and (e) when a result of the judgment of whether or not the acquired first visit information matches the stored second visit information is positive, judges that the visit by the forwarding agent is authentic (Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**),**

wherein the authentication apparatus and the IC card perform a challenge-response authentication process using the certification information from the IC card and the stored authentication information (Ahlstrom, Paragraphs [0031], The system retrieves the access code stored on the card and determines if the access code matches a code stored in the database. The matching of codes is hereby interpreted as a challenge-response authentication process. Furthermore, the authentication information is the access code stored in authentication apparatus (see Ahlstrom, Paragraph [0028]), and the certification is the access code stored in the IC card.**),**

Ahlstrom does not teach:

Wherein the authentication information is a secret key,

wherein the IC card stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader,

wherein the IC card receives the challenge data from the authentication apparatus, generates encrypted response data by encrypting the challenge data using the first key, and outputs the encrypted response data to the authentication apparatus via the card reader, and

wherein the authentication apparatus receives the encrypted response data from the IC card, generates a second key by executing a function, which is identical to the one-way function, on the secret key, generates decrypted data by decrypting the encrypted response data using the generated second key, and performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Abraham teaches:

Wherein thee authentication information is a secret key (Abraham, Col. 3, Lines 4-8**),**

wherein the IC card stores a first key that is obtained by executing a one-way function on a key that is identical with the secret key (Abraham, Col. 3, Lines 4-8, The one-way function is the decryption process of a value to obtain a random number RN (see Abraham, Col. 3, Lines 23-25).**),**

wherein the authentication apparatus generates challenge data, and outputs the generated challenge data to the IC card via the card reader (Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader.**),**

wherein the IC card receives the challenge data from the authentication apparatus, generates encrypted response data by encrypting the challenge data using the first key, and outputs the generated response data to the authentication apparatus via the card reader (Abraham, Col. 3, Lines 25-28**), and**

wherein the authentication apparatus receives the encrypted response data from the IC card, generates a second key by executing a function, which is identical with the one-way function, on the secret key (Abraham, Col. 3, Lines 28-30, Where the terminal 20 decrypts the value Z with the secret key in order to obtain a value A. Since the secret keys are the same, the one-way functions are also the same.**), generates decrypted data by decrypting the response data using the second key (**Abraham, Col. 3, Lines 28-30**), and performs an authentication by judging whether or not the generated decrypted data matches the challenge data (**Abraham, Col. 3, Lines 30-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 5, Ahlstrom in view of Abraham further teaches:

The first visit information is first time information that indicates a first time period for the visit by the forwarding agent (Ahlstrom, Paragraph [0035]**),**

wherein the second visit information is second time information that indicates a second time period for the visit by the forwarding agent (Ahlstrom, Paragraph [0035], The system is programmed to know, based on the access code, whether or not the card has a time restriction on it. Multiple time restrictions, i.e. time of day or number of times to visit, is second time information.**), and**

wherein the authentication apparatus judges whether or not the first time information matches the second time information (Ahlstrom, Paragraph [0035], Also in Paragraph [0031] the system determines if the access code retrieved from the IC card matches the access codes stored in the main unit.**).**

Claim 6, Ahlstrom in view of Abraham further teaches:

The first visit information is first business information that indicates a first business of the visit by the forwarding agent (Ahlstrom, Paragraph [0035], Temporary cards are programmed to only work for a certain time period, or for a certain number of times. Thus, the time periods and times are also considered as the business of the visit, because it signifies to the system that the user wants entry to the area in a specified time period The term “business” is here interpreted as meaning “purpose”.**),**

wherein the second visit information is second business information that indicates a second business of the visit by the forwarding agent (Ahlstrom, Fig. 1:

116, Paragraph [0031], The system selectively grants access based on the access code read from the card. The authentication apparatus has a list of authorized access codes (see Paragraph [0028]).**), and**

wherein the authentication apparatus judges whether or not the first business information matches the second business information (Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**).**

Claim 7, Ahlstrom in view of Abraham further teaches:

The first visit information includes (i) first time information that indicates a first time period for the visit by the forwarding agent and (ii) first business information that indicates a first business of the visit by the forwarding agent (Ahlstrom, Paragraph [0035], Because the system can recognize, based on the access code, when the user wishes to gain access to the door, the access code itself, which is first visit information, includes information embedded in it that indicates a time period and also business information.**),**

wherein the second visit information includes (iii) second time information that indicates a second time period for the visit by the forwarding agent and (iv) second business information that indicates a second business of the visit by the forwarding agent (Ahlstrom, Paragraphs [0031] and [0035], Because a list of access codes are stored at the authentication apparatus and the access codes are interpreted as first visit information, the list represents a list of second visit information that are the same values as the first visit information, which includes time information and business.**), and**

wherein the authentication apparatus judges whether or not the first time information matches the second time information, and judges whether or not the first business information matches the second business information (Ahlstrom, Paragraphs [0031] and [0035]**).**

Claim 12, Ahlstrom in view of Abraham further teaches:

The IC card further stores visitor information for identifying a visitor (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. Thus the IC card has a visitor information storage unit**), and**

wherein the authentication apparatus further acquires the visitor information from the IC card via the card reader (Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The authentication apparatus includes a visitor information acquiring unit, and the IC card has an output unit.**), and when the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the visitor information on a visitor information display unit (**Ahlstrom, Paragraph [0036]**).**

Claims 31, 46, and 47, Ahlstrom teaches:

An authentication apparatus, method, and an authentication program for verifying authenticity (Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card.**) of a visit by a forwarding agent using a portable recording medium of the forwarding agent (**Ahlstrom, Paragraph [0031], A card read by a card reader is a portable recording medium, and the user is a forwarding agent.**), the authentication apparatus being provided in a residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building. The system can be implemented in a place of residence (see Ahlstrom, Paragraph [0026]).**) of a person who is visited by the forwarding agent (**Ahlstrom, Paragraph [0026], Ahlstrom further discloses issuing temporary access cards, which is here interpreted as cards for people who only temporarily need access to the entrance by way of cards (see Paragraph [0035]). Therefore, these people may be interpreted as visitors.**), the authentication apparatus comprising:**

an information storage unit operable to store information for verifying the authenticity of the visit by the forwarding agent (Ahlstrom, Paragraph [0028]**); and**

a judgment unit operable to judge whether or not the visit by the forwarding agent is authentic by, via a card reader for reading the portable recording medium of the forwarding agent (Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit.**) and provided at an entrance of the residence**

(Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building.), **performing an authentication using information stored in the portable recording medium concerning the authenticity of the visit by the forwarding agent and using the stored information for verifying the authenticity of the visit by the forwarding agent (**Ahlstrom, Paragraph [0031]**),**

wherein the card reader detects a lock status of an entrance door of the residence (Ahlstrom, Paragraphs [0022] and [0030], The system has sensors to detect whether a door is opened or close. It is well-known in the art that doors in a controlled access system are locked when the door is closed, thus the sensors are capable of determining the lock status of the door.**),**

wherein the portable recording medium stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit by the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. The access codes are thus certification information stored on the IC card that is used to certify authenticity.**),**

wherein the information storage unit stores, as the information for verifying the authenticity of the visit by the forwarding agent, authentication information used to examine the certification information (Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card. The authentication apparatus has a list of authorized access codes (see Paragraph [0028]).**),**

wherein, when the card reader detects that the entrance door is locked, the judgment unit performs, via the card reader, the authentication by a challenge-response authentication process (Ahlstrom, Paragraphs [0031], The system retrieves the access code stored on the card and determines if the access code matches a code stored in the database. The matching of codes is hereby interpreted as a challenge-response authentication process. Furthermore, the authentication information is the access code stored in authentication apparatus (see Ahlstrom, Paragraph [0028]), and the certification is the access code stored in the IC card.**) using the certification information from the portable recording medium and the stored authentication information to judge whether or not the visit by the forwarding agent is authentic (**Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**),**

wherein the portable recording medium further stores, as the information concerning the authenticity of the visit, first visit information that indicates a business of the visit by the forwarding agent (Ahlstrom, Paragraph [0035], Temporary cards are programmed to only work for a certain time period, or for a certain number of times. Thus, the time periods and times are also considered as the business of the visit, because it signifies to the system that the user wants entry to the area in a specified time period The term "business" is here interpreted as meaning "purpose".**),**

wherein the information storage unit further stores, as the information for verifying the authenticity of the visit by the forwarding agent, second visit information used to examine the first visit information (Ahlstrom, Paragraph [0035], The system is programmed to recognize an access code as having time restrictions, thus the access code also serves as information concerning authenticity. The time restrictions are thus second visit information, and the access codes are stored in the main unit (see Paragraph [0028]).**),**

wherein, when a result of the authentication using the certification information from the portable recording medium and the stored authentication information is positive, the judgment unit (a) acquires the first visit information from the portable recording medium via the card reader, (b) judges whether or not the acquired first visit information matches the stored second visit information, and (c) when a result of the judgment of whether or not the acquired first visit information matches the stored second visit information is positive, judges that the visit by the forwarding agent is authentic (Ahlstrom, Paragraph [0035], The card reader retrieves the code from the card (see Paragraph [0031]), the system then determines if the code is valid, and then the system further determines from the retrieved code whether the card corresponds to a specific time restriction.**),**

Ahlstrom does not teach:

wherein the authentication information is a secret key,

wherein the portable recording medium stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the judgment unit generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader, and

wherein, upon receiving encrypted response data, which is generated by encrypting the challenge data using the first key, from the portable recording medium via the card reader, the judgment unit (d) generates a second key by executing a function, which is identical to the one- way function, on the secret key, (e) generates decrypted data by decrypting the encrypted response data using the generated second key, and (f) performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Abraham teaches:

Wherein the authentication information is a secret key (Abraham, Col. 3, Lines 4-8**),**

wherein the portable recording medium stores a first key that is obtained by executing a one-way function on a key that is identical with the secret key (Abraham, Col. 3, Lines 4-8, The one-way function is the decryption process of a value to obtain a random number RN (see Abraham, Col. 3, Lines 23-25).**),**

wherein the judgment unit generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader (Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader.**),**

wherein the IC card receives the challenge data from the authentication apparatus, generates encrypted response data by encrypting the challenge data using the first key, and outputs the generated response data to the authentication apparatus via the card reader (Abraham, Col. 3, Lines 25-28**), and**

wherein, upon receiving encrypted response data, which is generated by encrypting the challenge data using the first key, from the portable recording medium via the card reader, the judgment unit (d) generates a second key by executing a function, which is identical to the one- way function, on the secret key (Abraham, Col. 3, Lines 28-30, Where the terminal 20 decrypts the value Z with the secret key in order to obtain a value A. Since the secret keys are the same, the one-way functions are also the same.**), (e) generates decrypted data by decrypting the encrypted response data using the generated second key (**Abraham, Col. 3, Lines 28-30**), and (f) performs the authentication by judging whether or not the generated decrypted data matches the challenge data (**Abraham, Col. 3, Lines 30-34**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 36, Ahlstrom in view of Abraham further teaches:

The portable recording medium further stores therein visitor information for identifying a visitor (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. Thus the IC card has a visitor information storage unit.**), and**

wherein the authentication apparatus further comprises:

a visitor information acquiring unit operable to acquire the visitor information from the portable recording medium via the card reader (Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The authentication apparatus includes a visitor information acquiring unit, and the IC card has an output unit.**); and**

a visitor information display unit operable to display the visitor information when the judgment unit judges that the visit by the forwarding agent is authentic (Ahlstrom, Paragraph [0036]**).**

Claim 39, Ahlstrom teaches:

A portable recording medium of a forwarding agent (Ahlstrom, Paragraph [0031], A card read by a card reader is a portable recording medium, and the user is a forwarding agent.**) and used by an authentication apparatus to verify authenticity of a visit by the forwarding agent (**Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card.**), the authentication apparatus being provided in a residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building. The system can be implemented in a place of residence (see Ahlstrom, Paragraph [0026]).**) of a person visited by the forwarding agent (**Ahlstrom, Paragraph [0026], Ahlstrom further discloses issuing temporary access cards, which is here interpreted as cards for people who only temporarily need access to the entrance by way of cards (see Paragraph [0035]). Therefore, these people may be interpreted as visitors.**), the portable recording medium comprising:**

a storage unit operable to store, in advance, at least one piece of information concerning the authenticity of the visit by the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**);**

a receiving unit operable to receive first data from the authentication apparatus via a card reader (Ahlstrom, Paragraph [0031], The system verifies the access code stored on the portable medium. Thus, the card reader interrogation signal, as is known in the art, to the smart card is a first data from the input/output apparatus.**)** **provided at an entrance of the residence (**Ahlstrom, Fig. 1: 112, 114, Paragraph [0022], As can be seen from Figure 1, the card readers 112 and 114 are located adjacent to the gate 108 of the building.**);**

a data generating unit operable to generate second data from the first data using the information concerning the authenticity of the visit by the forwarding agent and stored in the storage unit, the second data being used for an authentication process (Ahlstrom, Paragraph [0031], The portable recording medium returns data stored on the smart card to the authentication apparatus in response to the interrogation signal of the card reader. The response is thus second data.**); and**

an output unit operable to output the second data to the authentication apparatus via the card reader (Ahlstrom, Paragraph [0031], It is well-–known in the art that smart cards are able to respond to interrogation signals by using an input/output device, depending upon the type of smart card used.**),**

wherein the storage unit stores, as the information concerning the authenticity of the visit by the forwarding agent, certification information that certifies the authenticity of the visit of the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. The access codes are thus certification information stored on the IC card that is used to certify authenticity.**),**

wherein the data generating unit generates the second data using the certification information (Ahlstrom, Paragraph [0031], The portable recording medium returns data stored on the smart card to the authentication apparatus in response to the interrogation signal of the card reader. The response is thus second data.**),**

wherein the storage unit further stores, as the information concerning the authenticity of the visit by the forwarding agent, visit information that indicates a business of the visit by the forwarding agent (Ahlstrom, Paragraph [0035], Temporary cards are programmed to only work for a certain time period, or for a certain number of times. Thus, the time periods and times are also considered as the business of the visit, because it signifies to the system that the user wants entry to the area in a specified time period The term "business" is here interpreted as meaning "purpose".**),**

wherein the output unit further outputs the visit information to the authentication apparatus via the card reader (Ahlstrom, Paragraph [0031], It is well-–known in the art that smart cards are able to respond to interrogation signals by using an input/output device, depending upon the type of smart card used.**),**

wherein the authentication apparatus stores authentication information used to examine the certification information (Ahlstrom, Fig. 1: 116, Paragraph [0031], The system selectively grants access based on the access code read from the card. The authentication apparatus has a list of authorized access codes (see Paragraph [0028]).**),**

wherein the authentication apparatus and the portable recording medium perform a challenge-response authentication process using the certification information from the portable recording medium and the stored authentication information (Ahlstrom, Paragraphs [0031], The system retrieves the access code stored on the card and determines if the access code matches a code stored in the database. The matching of codes is hereby interpreted as a challenge-response authentication process. Furthermore, the authentication information is the access code stored in authentication apparatus (see Ahlstrom, Paragraph [0028]), and the certification is the access code stored in the IC card.**),**

Ahlstrom does not teach:

Wherein the authentication information is a secret key,

wherein the storage unit stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key,

wherein the judgment unit generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader,

wherein the data generating unit receives the challenge data from the authentication apparatus, and generates encrypted response data by encrypting the received challenge data using the first key,

wherein the output unit outputs the encrypted response data to the authentication apparatus via the card reader, and

wherein, upon receiving the encrypted response data from the portable recording medium, the authentication apparatus (a) generates a second key by executing a function, which is identical to the one-way function, on the secret key, (b) generates decrypted data by decrypting the encrypted response data

using the generated second key, and (c) performs the authentication by judging whether or not the generated decrypted data matches the challenge data.

Abraham teaches:

Wherein the authentication information is a secret key (Abraham, Col. 3, Lines 4-8**),**

wherein the storage unit stores a first key that is obtained by executing a one-way function on a key that is identical to the secret key (Abraham, Col. 3, Lines 4-8, The one-way function is the decryption process of a value to obtain a random number RN (see Abraham, Col. 3, Lines 23-25).**),**

wherein the judgment unit generates challenge data, and outputs the generated challenge data to the portable recording medium via the card reader (Abraham, Col. 3, Lines 13-21, Terminal 20 transmits and receives information to and from the card, respectively, and thus is interpreted as a card reader.**),**

wherein the data generating unit receives the challenge data from the authentication apparatus, and generates encrypted response data by encrypting the received challenge data using the first key (Abraham, Col. 3, Lines 25-28**), and**

wherein the output unit outputs the encrypted response data to the authentication apparatus via the card reader (Abraham, Col. 3, Lines 25-28**), and**

wherein, upon receiving the encrypted response data from the portable recording medium, the authentication apparatus (a) generates a second key by executing a function, which is identical to the one-way function, on the secret key

(Abraham, Col. 3, Lines 28-30, Where the terminal 20 decrypts the value Z with the secret key in order to obtain a value A. Since the secret keys are the same, the one-way functions are also the same.), **(b) generates decrypted data by decrypting the encrypted response data using the generated second key** (Abraham, Col. 3, Lines 28-30), **and (c) performs the authentication by judging whether or not the generated decrypted data matches the challenge data** (Abraham, Col. 3, Lines 30-34).

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a challenge response authentication system as taught by Abraham.

The motivation would be to protect useful information by first authenticating all components in an authentication system (see Abraham, Col. 1, Lines 63-66).

Claim 43, Ahlstrom in view of Abraham further teaches:

A visitor information storage unit operable to store visitor information for identifying a visitor (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility. Thus the IC card has a visitor information storage unit),

wherein the output unit further outputs the visitor information to the authentication apparatus via the card reader (Ahlstrom, Paragraph [0022], The system has two card readers, one inside and one outside the building. The card readers are in communication with the main unit. The authentication apparatus includes a visitor information acquiring unit, and the IC card has an output unit.**).**

2. Claims 8-11, 35, and 42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Hill et al. (U.S. 6431453).

Claim 8, Ahlstrom in view of Abraham further teaches:

The IC card stores information identifying the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**) and displays information read from the IC card (**Ahlstrom, Paragraph [0036]**).**

Ahlstrom does not teach:

The IC card further stores article information concerning an article delivered by the forwarding agent, and

the authentication apparatus and an article information acquiring unit further acquires the article information from the IC card via the card reader, and when the authentication apparatus judges that the visit by the forwarding agent is authentic, displays the article information using an article information display unit.

Hill teaches:

The IC card further stores article information concerning an article delivered by the forwarding agent (Hill, Col. 3, Lines 30-35, Where the information stored on the IC chip 32 is account information, as is known in the prior art (see Hill, Col. 1, Lines 39-44). The IC card thus has an article information storage unit**), and**

the authentication apparatus and further acquires the article information from the IC card via the card reader, and authenticates the article information (Hill, Col. 4, Lines 20-27, The authentication apparatus has an article information acquiring unit, and also an output unit.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by integrating the teaching of storing information about a carrier as taught by Hill to be displayed on a display.

The motivation would be to increase the overall security to residents of the system by providing a way to verify packages being delivered by using known data storage capabilities of IC cards (see Hill, Col. 1, Lines 28-44). One of ordinary skill will recognize that allowing the system to verify information, such as the recipient of the package, would help identify the package prior to opening.

Claim 9, Ahlstrom in view of Abraham, and further in view of Hill further teaches:

The article information is a name of a sender of the article (Hill, Col. 1, Lines 28-44, It would have been obvious to one of ordinary skill in the art that the name of the sender, such as the vendor of a product, would be considered account information.**),** **and**

wherein the authentication apparatus acquires the name of the sender from the IC card (Hill, Col. 4, Lines 20-27**) and displays the acquired name (**Ahlstrom, Paragraph [0036]**).**

Claim 10, Ahlstrom in view of Abraham, and further in view of Hill further teaches:

The article information is a name of the article (Hill, Col. 1, Lines 28-44, It would have been obvious to one of ordinary skill in the art that the name of the article, such as the name of a product, would be considered account information.**), and**

wherein the authentication apparatus acquires the name of the article from the IC card (Hill, Col. 4, Lines 20-27**) and displays the acquired name of the article (**Ahlstrom, Paragraph [0036]**).**

Claim 11, Ahlstrom in view of Abraham, and further in view of Hill further teaches:

The article information is a message from a sender of the article (Hill, Col. 1, Lines 28-44, It would have been obvious to one of ordinary skill in the art that a message from a sender of the article, such as advertising or product information from a vendor, would be considered account information.**), and**

wherein the authentication apparatus acquires the message from the IC card (Hill, Col. 4, Lines 20-27**) and displays the acquired message (**Ahlstrom, Paragraph [0036]**).**

Claim 35, Ahlstrom in view of Abraham teaches:

The portable recording medium further stores article information identifying the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**) and displays information read from the portable recording medium (**Ahlstrom, Paragraph [0036]**).**

Ahlstrom in view of Abraham does not teach:

The portable recording medium further stores article information concerning an article delivered by the forwarding agent, and

wherein the authentication apparatus further comprises:

an article information acquiring unit further acquires the article information from the portable recording medium via the card reader, and

an article information display unit operable to display the article information when the judgment unit judges that the visit by the forwarding agent is authentic.

Hill teaches:

The portable recording medium further stores article information concerning an article delivered by the forwarding agent (Hill, Col. 3, Lines 30-35, Where the information stored on the IC chip 32 is account information, as is known in the prior art (see Hill, Col. 1, Lines 39-44). The IC card thus has an article information storage unit**), and**

an article information acquiring unit further acquires the article information from the portable recording medium via the card reader, and authenticates the article information (Hill, Col. 4, Lines 20-27, The authentication apparatus has an article information acquiring unit, and also an output unit.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by integrating the teaching of storing information about a carrier as taught by Hill to be displayed on a display.

The motivation would be to increase the overall security to residents of the system by providing a way to verify packages being delivered by using known data storage capabilities of IC cards (see Hill, Col. 1, Lines 28-44). One of ordinary skill will recognize that allowing the system to verify information, such as the recipient of the package, would help identify the package prior to opening.

Claim 42, Ahlstrom in view of Abraham further teaches:

The portable recording medium further stores article information identifying the forwarding agent (Ahlstrom, Paragraph [0031], The cards have access codes on them, which is used to determine accessibility.**) and displays information read from the portable recording medium (**Ahlstrom, Paragraph [0036]**).**

Ahlstrom in view of Abraham does not teach:

An article information storage unit operable to store article information concerning an article delivered by the forwarding agent, and

wherein the output unit further outputs the article information to the authentication apparatus via the card reader.

Hill teaches:

An article information storage unit operable to store article information concerning an article delivered by the forwarding agent (Hill, Col. 3, Lines 30-35, Where the information stored on the IC chip 32 is account information, as is known in the prior art (see Hill, Col. 1, Lines 39-44). The IC card thus has an article information storage unit**), and**

wherein the output unit further outputs the article information to the authentication apparatus via the card reader (Hill, Col. 4, Lines 20-27, The authentication apparatus has an article information acquiring unit, and also an output unit.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by integrating the teaching of storing information about a carrier as taught by Hill to be displayed on a display.

The motivation would be to increase the overall security to residents of the system by providing a way to verify packages being delivered by using known data storage capabilities of IC cards (see Hill, Col. 1, Lines 28-44). One of ordinary skill will recognize that allowing the system to verify information, such as the recipient of the package, would help identify the package prior to opening.

3. Claim 13 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Kinugasa et al. (U.S. 5898165).

Claim 13, Ahlstrom in view of Abraham does not teach:

The visitor information is a name of the visitor, and

the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor.

Kinugasa teaches:

Storing the name of a person on an IC card (Kinugasa, Col. 4, Lines 33-35**), and**

the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor (Kinugasa, Col. 4, Lines 27-35**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by incorporating the teaching of storing the name of a person into an IC card as taught by Kinugasa.

The motivation would be to provide addition information to further verify the identity of the person wanting access to the building. One of ordinary skill in the art would recognize that having more data fields for verification would improve the ability of the system to identify a person, thus improving the overall security of the system.

4. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Yasuda et al. (U.S. 4703347).

Claim 14, Ahlstrom in view of Abraham does not teach:

The visitor information is an image of a facial photo of the visitor, and

the authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo.

Yasuda teaches:

Storing an image of a facial photo of a person in an IC card (Yasuda, Col. 3, Lines 23-29**), and**

wherein an authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo (Yasuda, Col. 3, Lines 35-42**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by incorporating the teaching of storing a photo of a person into an IC card as taught by Yasuda.

The motivation would be to provide a more reliable way to identify a person using individuality discriminating information (see Yasuda, Col. 2, Lines 20-30).

5. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), further in view of Kinugasa et al. (U.S. 5898165), and further in view of Yasuda et al. (U.S. 4703347).

Claim 15, Ahlstrom in view of Abraham does not teach:

The visitor information is a name and an image of a facial photo of the visitor, and

the authentication apparatus acquires the name and the image of the facial photo of the visitor from the IC card and displays the acquired name and image of the facial photo.

Kinugasa teaches:

Storing the name of a person on an IC card (Kinugasa, Col. 4, Lines 33-35**), and**

the authentication apparatus acquires the name of the visitor from the IC card and displays the acquired name of the visitor (Kinugasa, Col. 4, Lines 27-35**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom by incorporating the teaching of storing the name of a person into an IC card as taught by Kinugasa.

The motivation would be to provide addition information to further verify the identity of the person wanting access to the building. One of ordinary skill in the art would recognize that having more data fields for verification would improve the ability of the system to identify a person, thus improving the overall security of the system.

Ahlstrom in view of Abraham, and further in view of Kinugasa does not teach:

The visitor information is a facial photo, and the authentication apparatus acquires the image of the facial photo.

Yasuda teaches:

Storing an image of a facial photo of a person in an IC card (Yasuda, Col. 3, Lines 23-29**), and**

an authentication apparatus acquires the image of the facial photo of the visitor from the IC card and displays the acquired image of the facial photo (Yasuda, Col. 3, Lines 35-42**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the smart card in Ahlstrom in view of Kinugasa by incorporating the teaching of storing a photo of a person into an IC card as taught by Yasuda.

The motivation would be to provide a more reliable way to identify a person using individuality discriminating information (see Yasuda, Col. 2, Lines 20-30).

6. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Yasukura (U.S. 6990588).

Claim 30, Ahlstrom in view of Abraham teaches:

The authentication apparatus further stores an apparatus identifier for identifying the authentication apparatus (Ahlstrom, Paragraph [0028], The apparatus identifier is an access code which grants access to tenants. Because the codes are unique to the system, the access codes identify the authentication apparatus itself.**).**

Ahlstrom in view of Abraham does not teach:

The authentication apparatus outputs the apparatus identifier to the IC card via the card reader when the authentication apparatus judges that the visit by the forwarding agent is authentic, and

wherein the IC card, upon receiving the apparatus identifier from the authentication apparatus, stores the received apparatus identifier.

Yasukura teaches:

The authentication apparatus outputs the apparatus identifier to the IC card via the card reader when the authentication apparatus judges that the visit by the forwarding agent is authentic (Yasukura, Col. 31, Lines 25-40, When a user wishes to update the information stored on the IC card, the user must first be authenticated. Once authenticated, the user may erase old identification information.**), and**

wherein the IC card, upon receiving the apparatus identifier from the authentication apparatus, stores therein the received apparatus identifier (Yasukura, Col. 31, Lines 35-40, The user enters updated information to be written on the IC card.**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by integrating the teaching of rewriting on an IC card as taught by Yasukura.

The motivation would be to ensure that authorized personnel will continue to have access to an access controlled system in case identification information has changed over time, such as biometric information, access code changes, etc.

7. Claim 38 and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ahlstrom et al. (U.S. 2003/0081747) in view of Abraham et al. (U.S. 4799061), and further in view of Gobburu et al. (U.S. 2002/0060246).

Claims 38 and 45, Ahlstrom in view of Abraham does not teach:

The authentication apparatus is a mobile phone.

Gobburu teaches:

A mobile phone with a built-in smart card reader (Gobburu, Paragraph [0082]**).**

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the access control system in Ahlstrom by incorporating the teaching of a mobile phone with a built-in smart card reader as taught by Gobburu.

The motivation would be to provide a wireless communications device capable of performing authentication, which would increase the range of the transmission of data since it is well-known in the art that mobile phones use cellular towers to transmit information over long distances. Furthermore, a mobile phone would allow the system to be placed anywhere, and not necessarily be affixed to the entrance of a residence.

Response to Arguments

Applicant's arguments filed 04/27/2010 have been fully considered but they are not persuasive.

In response to applicant's arguments on Page 23, that neither the Ahlstrom nor the Abraham references teaches a "one-way function", the examiner respectfully disagrees. First, based on the interpretation of the claim language, a challenge-response is two-way communication, because the authentication apparatus challenges the IC card, and then the IC card outputs an encrypted response. Each transmission, i.e. the challenge or response by itself, represents a one-way communication, but the authentication method performs both a challenge and response. Second, the Abraham reference teaches transmitting a challenge, in the form of an encrypted random number to be authenticated by the tag. The tag then decrypts the communication, and transmits a response to the challenge to the terminal to be authenticated (see Abraham, Col. 3, Lines 10-34). Each transmission, the challenge or response, is performed using one-way communication.

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JAMES YANG whose telephone number is 571-270-5170. The examiner can normally be reached on M-F 8:30-5 EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian Zimmerman can be reached on 571-272-3059. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/J.Y./

/Brian A Zimmerman/
Supervisory Patent Examiner, Art Unit 2612